

involved in the appeal, referring to the specification by page and line number, and to the drawings by reference characters. Moreover, Appellants respectfully submit that both the original and the replacement "Summary of Claimed Subject Matter" include a first paragraph that concisely explains the subject matter of the independent claims.


Accordingly, Appellants submit that the attached paper is fully responsive to the Notice and corrects any deficiencies in the Appeal Brief. Appellants respectfully request that the Office accept the attached paper for consideration with the Appeal Brief.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 20, 2006

By: 

Arthur A. Smith
Reg. No. 56,877
/phone number: (202) 408-4049/

Attachment: Replacement Section for "Summary of Claimed Subject Matter"

V. SUMMARY OF CLAIMED SUBJECT MATTER (REPLACEMENT SECTION)

The claimed subject matter on appeal prevents electronic data, such as music data, video data, or software programs from being illegally copied. A memory has a data storage area divided into a plurality of blocks. Each block is divided into sectors, and a different encryption key encrypts each sector.

Independent claim 1 recites an information recording device (Fig. 2, element 200) for executing processing which stores data to a memory (*Specification*, p. 24, lines 7-21; Fig. 2, elements 210 and 220). The memory having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3a), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity where M represents a natural number (*Specification*, p. 27, lines 1-7). The information recording device comprising a cryptosystem unit (Fig. 4, element 320) that selectively uses a different encryption key (see, e.g., encryption keys stored in memory unit 321 illustrated in Fig. 4; Fig. 8B; Fig. 27B; Fig. 29) for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors (*Specification*, p. 80, line 16 - p. 82, line 11). Wherein the data includes a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 43, lines 5-23 and p. 85, lines 1-6) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321

illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification* p. 46, lines 2-12). An integrity checking unit (Fig. 2, element 204) for checking the integrity of the revocation list and the block permission table (*Specification*, p. 28, lines 17-24 and p. 51, line 18 - p. 52, line 12).

Independent claim 8 recites an information playback device (Fig. 2, element 200) for executing processing which reads data from a memory (*Specification*, p. 24, lines 7-21; Fig. 2, elements 210 and 220). The memory having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3a), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 27, lines 1-7). The information playback device comprising a cryptosystem unit (Fig. 4, element 320) which selectively uses a different decryption key (see, e.g., encryption keys stored in memory unit 321 illustrated in Fig. 4; Fig. 8B; Fig. 27B; Fig. 29) for each sector from the first sector to the M-th sector to execute decryption processing and the cryptosystem unit executes decryption processing on data stored in each of the sectors (*Specification*, p. 103, line 6 - p. 105 line 17). Wherein the data includes a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 43, lines 5-23 and p. 95, lines 10-18) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that

describes memory access control information (*Specification*, p. 46, lines 2-12 and p. 100, line 23 - p. 101, line 8). An integrity checking unit (Fig. 2, element 204) for checking the integrity of the revocation list and the block permission table (*Specification*, p. 28, lines 17-24 and p. 95, line 12 - p. 96, line 11).

Independent claim 15 recites an information recording medium (Fig 2, elements 210 and 230) having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (*Specification* p. 26, lines 16-24; and Fig. 3). Each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 27, lines 1-7). Wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area, (*Specification*, p. 36, line 18 - p. 38, line 21; p. 40, line 1 - p. 41, line 4; Figs. 6B and 7). Wherein the storage area stores data including a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 43, line 5 - p. 44, line 6) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification* p. 46, lines 2-12). Wherein an integrity check of the integrity of the revocation list and block permission table is performed (*Specification*, p. 51, line 18 - p. 52, line 12).

Independent claim 17 recites an information recording method (Figs. 41 and 42) for executing processing which stores data to a memory (Fig 2, elements 210 and 230) having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 108, lines 7-10 and p. 112, lines 13-24). The information recording method comprising encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector (*Specification*, p. 108, lines 7-13). Storing data including a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 106, line 11 - p. 107, line 15) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification* p. 46, lines 2-12). Performing an integrity check of the revocation list and the block permission table (*Specification*, p.113, lines 5-16).

Independent claim 24 recites an information playback method (Figs. 35 and 36) for executing processing which reads data from a memory (Fig 2, elements 210 and 230) having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3), each of the blocks consists of M sectors (Fig. 3b) from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 93, lines 10-21). The information

playback method comprising decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector (*Specification*, p. 96, lines 19-25). Storing data including a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 94, line 12 - p. 95, line 9) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification*, p. 46, lines 2-12). Performing an integrity check of the revocation list and the block permission table (*Specification*, p. 100, line 23 - p. 102, line 21).

Independent claim 31 recites a computer-readable medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising storing data in a memory (Fig 2, elements 210 and 230) having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3), each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 108, lines 7-10 and p. 112, lines 13-24). Encryption processing data to be stored in the sectors by performing encryption using a different encryption key for each sector from the first sector to the M-th sector (*Specification*, p. 108, lines 7-13). Storing data including a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information

regarding revoked media or content (*Specification*, p. 106, line 11 p. 107, line 15) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification*, p. 46, lines 2-12).

Checking the integrity of the revocation list and the block permission table.

(*Specification*, p. 113, lines 5-16).

Independent claim 32 recites a computer readable medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising reading data from a memory (Fig 2, elements 210 and 230) having a data storage area (Fig. 2, elements 212 and 232) consisting of a plurality of blocks (Fig. 3), each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (*Specification*, p. 93, lines 10-21). Decrypting data stored in each of the sectors by executing decryption processing using a different decryption key for each sector from the first sector to the M-th sector (*Specification*, p. 96, lines 19-25). Storing data including a revocation list (see, e.g., revocation list storage area of memory unit 321 illustrated in Fig. 2; revocation list storage area of memory unit 321 illustrated in Fig. 4; and Fig. 9) having revocation information regarding revoked media or content (*Specification*, p. 94, line 12 - p. 95, line 9) and a block permission table (see, e.g., block permission table (BPT) storage area of memory unit 321 illustrated in Fig. 4; Fig. 10; and Fig. 13) for accessing a permission table that describes memory access control information (*Specification*, p. 46, lines 2-12). Checking the integrity of the revocation list and the block permission table. (*Specification*, p. 100, line 23 - p. 102, line 21).